Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/AU05/000364

International filing date: 15 March 2005 (15.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: AU
Number: 2004201058
Filing date: 15 March 2004 (15.03.2004)

Date of receipt at the International Bureau: 10 May 2005 (10.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/AU2005/000364

Australian Government

Patent Office
Canberra

I, JANENE PEISKER, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Complete specification in connection with Application No. 2004201058 for a patent by LOCKSTEP CONSULTING as filed on 15 March 2004.

WITNESS my hand this
Second day of May 2005

JANENE PEISKER
TEAM LEADER EXAMINATION
SUPPORT AND SALES

Title

Means and method of issuing Anonymous Public Key Certificates for indexing electronic record systems.

Technical field

The invention disclosed herein relates generally to electronic record systems and in particular relates to the unambiguous identification of registered persons in said systems to whom said records pertain. Registered persons in many electronic record systems may wish to remain anonymous so that their private records are not readily identifiable by unauthorised persons as belonging to said registered persons. This invention is well suited to applications where Public Key Infrastructure is used as an authentication method for electronic records management. The invention is particularly well suited to applications where smartcards or similar portable personal computing devices are used to control asymmetric cryptographic Private Keys within said Public Key Infrastructure. A preferred embodiment of this invention is disclosed which relates particularly to the field of electronic health records.

Background art

As will be seen, a preferred embodiment of the invention disclosed herein relates particularly to the field of electronic health records. While the present invention is not restricted to application in electronic health record systems, certain problems common in electronic health record systems are particularly illustrative of the more general problems overcome by the invention. Therefore pertinent background art from the field of electronic health record systems will now be described for the purpose of illustrating, without limitation, the important principles of the present invention.

Electronic health record systems use computer memory stores to retain information relating generally to the healthcare and medical episodes of patients. Users of electronic health record systems may include, without limitation, patients, primary care doctors, clinical specialists, hospital doctors, acute care nurses, community nurses, medical researchers, healthcare managers, healthcare

policy analysts, and agents of health insurance companies. Electronic health record systems bring a range of benefits to patients, to authorised users and to healthcare systems generally including easier and/or faster access to important healthcare information at the point of clinical care where treatment is being delivered to patients, improved clinical outcomes resulting from better quality information being available at the point of clinical care, less frequent re-admissions to hospital as a result of better information being available to primary healthcare providers, reduced costs associated with the gathering of redundant clinical information, reduced costs associated with re-keying of clinical information from paper records, and enhanced quality of healthcare across the entire healthcare system resulting from continuous improvement to treatment modalities made possible by accumulated performance data.

Electronic health record systems generally require patients to be unambiguously identified so that authorised users with a legitimate interest in a given patient may reliably access information pertaining to that patient and to that patient alone.

It will be appreciated by persons skilled in the field of electronic health record systems that said systems can generally be constructed in a range of ways in respect of the degree of centralisation of the component data items that together constitute the whole of a given person's electronic health record. It is possible to construct an electronic health record system where all component data items relating to each patient (or a significant majority of the component data items relating to each patient) are stored within a substantially single centralised computer memory store. Further, it is possible to construct an electronic health record system where component data items relating to each patient are stored separately within a plurality of different decentralised computer memory stores. Users of decentralised electronic health record systems may benefit from search engine computer software which may automatically locate data items pertaining to a given patient wherever said records are located across the plurality of computer memory stores, and additional computer software which may subsequently collate, process and/or present to the user information from said component data items.

Whether an electronic health record system is constructed to use centralised memory storage or to use decentralised memory storage, it generally remains an important requirement that each patient be unambiguously identified.

Electronic health record systems generally include an access control function which serves to restrict the type of information, amount of information and/or degree of detail of information made available to different types of users. As is generally understood by those skilled in the field of electronic health records, different types of users have different needs in respect of the information they are entitled to exchange with an electronic health record system. Certain users may be authorised to write new information into the electronic health record of a given patient or to modify existing information relating to a patient, while other users may only be authorised to read information without modifying said information. Further, information retrieved from an electronic health record system may or may not be de-identified before being made available to certain types of user who have requested said information.

In general, authorised healthcare providers with a direct clinical interest in a patient may be entitled to access identifiable patient information pertaining to that patient from an electronic health record. Said authorised healthcare providers may include without limitation primary care doctors, hospital doctors, specialist doctors, acute care nurses, community care nurses, medical diagnosticians, and allied health workers. Non-clinical health system workers with no direct clinical interest in patients may nevertheless have legitimate interests in de-identified electronic health records for purposes including without limitation population health research, epidemiological investigation, compilation of evidence as to the efficacy of given healthcare protocols, and analysis of cost-benefit data across health systems. Said non-clinical health system workers may include without limitation academic researchers, public policy analysts, authorised civil servants from public health systems, human resources professionals, and authorised administrators of healthcare institutions. The access control function of an electronic health record will generally be designed to include a categorisation scheme for authorised users and will apply said scheme when processing requests from users to access information within the electronic health record system.

Health authorities generally issue members of the public with unique health system identification numbers. Said identification numbers may be printed on the surface of a health system identification card ("Health Id Card") together with the name of the person ("Card Holder") to whom the identification number has been issued. As is generally known, different health systems make use of different types of card technologies to convey health system identification numbers, including paper, cardboard or plastic cards. Plastic Health Id Cards may additionally feature magnetic stripe memory storage and/or integrated circuit memory storage. Said additional memory storage may be used to store the name of the Health Id Card Holder, the health system

identification number of said Card Holder and/or other information about said Card Holder. Information so stored in magnetic stripe memory or integrated circuit memory is thereby more readily available to healthcare computer systems with which said Health Id Card may be used at the time and place healthcare services are provided.

Health Id Cards as described may be issued and distributed by government authorities and used widely across national health systems. National Health Id Card systems are especially well known in relation to the management of public health insurance entitlements and payments. Independent Health Id Card systems may additionally be created by commercial organisations such as private health insurers, by regional or local government healthcare authorities, and/or by healthcare institutions such as hospitals. The present invention is equally applicable to singular Health Id Card systems and to plural Health Id Card systems.

In order to maximise patient privacy, designers of electronic health record systems generally seek to minimise the amount of identifiable personal information which is contained in each component data item of the electronic health record. Yet the need to index patient information generally requires that some type of record pointer information uniquely linked to the identity of said patient be stored within each component data item pertaining to that patient. This design requirement leads to a potential problem where if a person has access to an electronic health record and if said person additionally has knowledge of the linkage between patients' identities and their respective record pointer values, then said person can readily match component data items from said electronic health record with the identities of patients, thus identifying healthcare information which is otherwise intended to remain private and confidential.

It will be seen that the present invention overcomes the problem of ready identification of a patient from knowledge of said patient's electronic health record pointer values by making the linkage of the pointer value and the respective patient identity unavailable to all persons except for the patient.

The relatively high level of familiarity and widespread availability of many existing Health Id Card systems may appear to make them attractive options for indexing electronic health records. However, the re-use of existing health system identification numbers as pointers to index electronic health records can cause problems in respect of privacy. Health system identification numbers as printed on Health Id Cards become known to indeterminate numbers of people through the normal use of said cards over time in the healthcare system. Unscrupulous persons may make illicit copies

of patients' names together with matching health system identification numbers. Under these circumstances any electronic health record system which utilises health system identification numbers as pointers to index patient information will be vulnerable to unauthorised access by persons with knowledge of patient information from Health Id Cards. Thus it is generally understood by persons skilled in the field of electronic health records that existing health system identification numbers and Health Id Cards should not be used without significant modification as a method to index patient information in an electronic health record.

A further feature of certain electronic record systems is the use of Public Key Infrastructure as a method to authenticate users of said electronic record systems. As is generally known to persons skilled in the field of electronic security, Public Key Infrastructure refers broadly to the issuance of so-called Public Key Certificates to registered users in a defined transaction system, the usage in software programs of said Public Key Certificates as inputs to create so-called Digital Signatures which secure electronic transmissions and electronic data records, and the deployment of computer systems and management processes to facilitate the lifecycle maintenance of said Public Key Certificates.

A Public Key Certificate is generally an electronic document typically containing in a standardised format at least the following:

- information pertaining to the identity of the person or entity to whom the Public Key Certificate is issued (said person is known generally as the "Certificate Holder" and may also be known as the "Certificate Subject" or the "Certificate Subscriber")
- a copy of an asymmetric cryptographic Public Key assigned to said person to whom the Public Key Certificate is issued
- information pertaining to the identity of the entity which issued the Public Key Certificate (said issuing entity is known generally as a "Certification Authority")
- date and time information defining a Validity Period for the Public Key Certificate
- the Digital Signature of said Certification Authority.

Further it is generally understood that a Certification Authority may be assisted by one or more so-called Registration Authorities in respect of the process of issuing Public Key Certificates to Certificate Holders, said Registration Authorities being entities affiliated with said Certification Authority and which verify the identity and eligibility of persons applying to be issued with Public Key Certificates according to identification protocols and other conditions laid down by the

Certification Authority. Further it is generally understood that a Certification Authority may publish copies of Public Key Certificates together with other pertinent information in a generally available online repository so that parties to electronic transactions involving Certificate Holders may verify information provided by said Certificate Holders against the information published in said repository.

It will be generally known to persons skilled in the field of electronic security that the term Digital Signature refers generally to a computer generated code related to a given digital data item and created through the operation of a cryptographic algorithm on said data item in conjunction with a unique asymmetric cryptographic Private Key to which is linked a unique asymmetric cryptographic Public Key. Verification of the fact that a given Digital Signature code was created from a given data item may be performed through a further operation of a related cryptographic algorithm on said Digital Signature code in conjunction with said asymmetric cryptographic Public Key. If an asymmetric cryptographic Private Key is reliably under the control of a Public Key Certificate Holder and if the associated said Public Key is made known to another person then said person, following successful verification of a Digital Signature code and digitally signed data item in conjunction with said Public Key, may be able to ascribe said digitally signed data item to said Public Key Certificate Holder. An important purpose of Public Key Certificates is therefore to provide to persons using Public Key Infrastructure reliable and widely available evidence of the association between given Public Key Certificate Holders and their respective asymmetric cryptographic Public Keys and by extension the association between said Certificate Holders and their respective asymmetric cryptographic Private Keys.

In certain embodiments of Public Key Infrastructure the usability and security of asymmetric cryptographic Private Keys is enhanced by the storage of said Private Keys under the control of a portable personal computing device, one example of which is that commonly known as a smartcard.

Where Public Key Infrastructure is used within an electronic record system, certain events occurring in said system may be securely recorded with the aid of Digital Signatures of persons associated with said events. In particular where a given authorised user has originated a new data item to be written into the electronic record then said data item may be Digitally Signed by said authorised user. In the particular case of an electronic health record system where a given healthcare provider has originated a new data item pertaining to a given patient to be written into

the electronic record then said data item may be digitally signed by both said healthcare provider and said patient.

Public Key Infrastructure as generally understood and as described herein poses certain problems in respect of the privacy of persons whose personal information is contained in an electronic record system. In particular where Public Key Certificates are made generally available by Certificate Authorities via repositories it may be possible for unauthorised persons to readily identify Public Key Certificate Holders.

While not generally known, it is possible for so-called Anonymous Public Key Certificates to be created and issued which do not contain the name of the person to whom the certificate is issued. In order for said anonymous Public Key Certificates to be useful it is generally required that authorised users are able to link a given Anonymous Public Key Certificate holder to their Public Key Certificate.

It will be seen that the invention disclosed herein provides a method for securely effecting a link between a given Anonymous Public Key Certificate Holder and their Public Key Certificate where said link under normal circumstances is under the sole control of said Certificate Holder. Further it will be seen that the present invention provides a method for including within said Anonymous Public Key Certificates one or more computer memory pointers with which records pertaining to the Public Key Certificate Holder may be indexed from within an electronic record system.

Summary of the Invention

In one aspect, the invention disclosed herein provides a method of issuing Anonymous Public Key Certificates to Registered Persons whose personal information is held within an electronic record system, the method securely linking said Anonymous Public Key Certificates to portable personal computing devices issued respectively to the same said Registered Persons, said linking being effected by storing the asymmetric cryptographic Private Key associated with each said Anonymous Public Key Certificate under the control of said portable personal computing devices, and storing electronic record pointers within said Anonymous Public Key Certificates, so that said Registered Persons' records may variously be indexed identifiably using their name and/or other identity information, or alternatively indexed anonymously using said electronic record pointers; the method comprising the steps of:

- Issuing to each Registered Person whose personal information is held within an electronic record system a portable personal computing device with the ability to control the storage of one or more asymmetric cryptographic Private Keys.
- Visibly printing upon the surface of said personal computing device human readable identity information pertaining to said Registered Person, where said information without limitation may include the name of said Registered Person and/or other information as may be relevant to the management of records pertaining to said Registered Person.
- Generation of one or more pairs of matching asymmetric cryptographic Private and Public Keys.
- Storage of said asymmetric cryptographic Private Key(s) under the control of said portable personal computing device.
- Issuing to each said Registered Person an Anonymous Public Key Certificate for each asymmetric cryptographic Public Key which matches each said asymmetric cryptographic Private Key stored under the control of said portable personal computing device.
- Inclusion within the data contents of each said Anonymous Public Key Certificate one or more electronic record pointers which may be used to index records pertaining to said Registered Person stored within said electronic record system.

In a further aspect, this invention provides a means for issuing Anonymous Public Key Certificates to Registered Persons about whom personal information is held within an electronic record system, the means including electronic record pointers contained in said Anonymous Public Key Certificates, and linking said Anonymous Public Key Certificates to smartcards or similar portable personal computing devices capable of controlling the storage of asymmetric cryptographic Private Keys; the means comprising the elements of:
- One or more portable personal computing devices with the ability to each control the storage of one or more asymmetric cryptographic Private Keys.
- A recognised authoritative entity to issue said portable personal computing devices to Registered Persons whose personal information is held within said electronic record system.
- Human readable identity information pertaining to each said Registered Person visibly printed on the surface of respective said portable personal computing devices where said identity information without limitation may include the name of said Registered Person and/or other information as may be relevant to the management of records pertaining to said Registered Person.
- A key generation system to create asymmetric cryptographic Private and Public Keys.

- One or more Public Key Certificates issued to each said Registered Person and associated with respective asymmetric cryptographic Private Keys stored under the control of said portable personal computing devices.
- One or more electronic record pointers contained within the data contents of each said Public Key Certificate where said electronic record pointers may be used to index records within said electronic record system pertaining to the Registered Person to whom each said Public Key Certificate has been issued.
- A Certification Authority which creates said Public Key Certificates for said Registered Persons.
- One or more Registration Authorities which may assist the Certification Authority in producing Public Key Certificates, in particular by verifying the identity and eligibility of Registered Persons applying for Public Key Certificates.

A significant advantage of this invention is that the only direct linkage between each said Anonymous Public Key Certificate and the Registered Person to whom said Anonymous Public Key Certificate has been issued is through the asymmetric cryptographic Private Key associated with said Public Key Certificate. In keeping with generally understood principles of Public Key Infrastructure, the only operative instance of each said Private Key is stored under the control of a portable personal computing device issued to the Public Key Certificate Holder. Therefore the only direct means to link a Registered Person to their corresponding Anonymous Public Key Certificate is through said Registered Person's portable personal computing device which is understood to remain at all times under the control of said Registered Person. Using this invention, the retrieval of identifiable records pertaining to a given Registered Person from the electronic record system is normally only possible with the agency of said Registered Person's portable personal computing device and therefore with said Registered Person's consent.

Where an Anonymous Public Key Certificate containing an electronic record pointer is associated with an asymmetric cryptographic Private Key, it will be appreciated that any Digital Signature code created for a given data item by the Registered Person to whom said Anonymous Public Key Certificate has been issued has the effect of linking said data item to the value of said electronic record pointer associated with said Registered Person. Verification of said Digital Signature code using said Anonymous Public Key Certificate evinces the association of said electronic record pointer with both said data item and said Registered Person. Yet examination of said data item and said Anonymous Public Key Certificate will not reveal the identity of associated said Registered Person.

It will be seen that alternative means for accessing a given Registered Person's Anonymous Public Key Certificate is required in a practical electronic record system in order for legitimate non-consensual access to personal electronic records to be possible under emergency conditions and under other prescribed conditions as may apply for a particular electronic record system. Such means are described elsewhere in this specification.

In a preferred embodiment of this invention, said portable personal computing devices take the form of smartcards issued to said Registered Persons where upon the surface of each said smartcard is printed the name of corresponding said Registered Person together with such additional identity information as is deemed necessary by the designer of the electronic record system.

In a particularly preferred embodiment of this invention, a national healthcare authority deploys smartcards as patient identity cards where said smartcards have the capability to control the storage of one or more asymmetric cryptographic Private Keys. Said smartcards are not necessarily initially issued with said Private Key(s). At some later time each patient to whom a smartcard has been so issued may individually elect to have one or more asymmetric cryptographic Private Keys stored under the control of said smartcard and with corresponding Anonymous Public Key Certificates created on said patient's behalf. It will be understood by persons skilled in the field of electronic health record systems that an electronic record pointer value stored within said Anonymous Public Key Certificate may be what is commonly known as a Unique Patient Identifier.

Subsequently in this particularly preferred embodiment, healthcare providers with a direct clinical interest in said patient may with said patient's cooperation and consent, use said patient's smartcard to identifiably exchange information pertaining to said patient with an electronic health record system. Alternatively, other health system workers with no direct clinical interest in a patient may use a given anonymous electronic record pointer value to index anonymous or de-identified information for said patient from said electronic health record system. Further said electronic record pointer value may be stored within the data contents of the Anonymous Public Key Certificate which has been issued to said patient.

As is generally understood, electronic health record system actions such as writing new data to a given patient's record generally requires the consent of said patient together with the agency of an

authorised healthcare worker. In typical electronic health record systems, the healthcare worker must usually be authorised by the patient. In a preferred embodiment of the present invention, patient consent is unambiguously mediated by said patient undertaking certain prescribed actions with their portable personal computing device as appropriate to the design of the electronic health record system in use. As is generally understood by persons skilled in electronic security systems, portable personal computing devices may be pass-phrase protected such that the holder of such a portable personal computing device must first enter a secret pass-phrase known only to said holder into a computer workstation in order to activate said personal device. In a preferred embodiment therefore the fact of a given patient's consent for a healthcare provider to perform a certain action upon said patient's electronic health record is conveyed to the electronic health record system by the action of the patient deliberately using their portable personal computing device in conjunction with the healthcare provider's workstation and correctly entering their secret pass-phrase.

In a preferred embodiment the present invention allows for an explicit record to be made of patient consent as to each consensual action undertaken by a healthcare provider on said patient's electronic health record where each said record of consent is comprised of a Digital Signature code created using said patient's asymmetric cryptographic Private Key operating on a data item in said electronic health record which is representative of said consensual action.

An objective of the present invention is to provide for a linkage between a given Registered Person's identity and one or more Anonymous Public Key Certificates issued to said Registered Person where said linkage is only ordinarily available via the agency of said Registered Person's portable personal computing device. The present invention provides that identifiable access to information pertaining to a Registered Person from an electronic record system ordinarily requires said Registered Person to present their portable personal computing device to a workstation (such as by inserting said personal device into a reader or by having said personal device within range of a wireless scanner) and enter their secret pass-phrase into a computer workstation in order to activate said portable personal computing device. As has been mentioned previously in this specification, it may be necessary in a practical electronic record system for legitimate non-consensual access to personal electronic records to be made possible under emergency conditions or under other prescribed conditions as may apply for a particular electronic record system. In a preferred embodiment where the electronic health system is an electronic health record system and Registered Persons are patients whose personal health information is stored within said electronic health record system it may be important for emergency healthcare providers such as hospital

doctors to be able to retrieve identifiable information from an electronic health record system pertaining to a given patient when said patient is not competent to enter their secret pass-phrase into a workstation to activate their portable personal computing device. Those skilled in the field of electronic health record systems will appreciate that one example of such a scenario where a given patient may not be competent to enter their secret pass-phrase is where said patient has lost consciousness.

It will be appreciated by persons skilled in the design of electronic record systems and/or electronic security devices that in practical embodiments of the present invention there is a range of potential methods for archiving copies of electronic record pointers in such a way that said pointers may be linked to the identity of respective Registered Persons associated with said pointers. It is outside the scope of the invention as broadly described in this specification to describe said archiving methods in detail. In order only to demonstrate that the practical requirement for provision within the present invention of legitimate non-consensual access to a Registered Person's personal electronic records may be met, it is noted here that said archiving methods may without limitation include: transmission to a trusted third party copies of electronic record pointers and names of respective Registered Persons to whom said pointers relate and subsequent provision on request by duly authorised persons copies of said pointers corresponding to the names of given Registered Persons; or construction of portable personal computing devices with a facility to grant access to the Public Key Certificate memory store controlled by said portable personal computing devices by duly authorised persons entering an emergency access secret pass-phrase without said Registered Persons entering their own secret pass-phrase.

Brief description of the Drawings

An example of the invention embodied in the field of electronic health record systems will now be described with reference to the accompanying drawings, in which:

Figure 1 is a block diagram representing the distribution of Health ID Cards to Patients and the issuance of associated Anonymous Public Key Certificates to said Patients.

Figure 2 is a block diagram which, for the purposes of illustration, represents a plurality of Healthcare Providers with an interest in the one Patient, and a preferred method by which said Healthcare Providers may with said Patient's consent exchange identifiable personal information about said Patient with a plurality of electronic health record systems.

Figure 3 is a block diagram which, for the purposes of illustration, represents a plurality of non-clinical health system workers with no direct interest in any Patients, and a preferred method by which said non-clinical health system workers may access de-identified information about a given Anonymous Patient using said Patient's electronic health record pointer.

Figure 4 is a block diagram which, for the purposes of illustration, represents a Hospital Doctor attempting to provide emergency clinical treatment to a Non-Competent Patient, and a preferred method by which said Hospital Doctor may firstly retrieve said Non-Competent Patient's Anonymous Public Key Certificate using said Non-Competent Patient's name and/or other health system identity information, and secondly use a Health Record Pointer from said Anonymous Public Key Certificate to index said Non-Competent Patient's electronic health record.

Best mode of invention

The best mode of performing the invention will now be described in relation to an electronic health record system where Registered Persons are Patients carrying smartcard based Health ID Cards. However it will be recognised that the invention is equally applicable to other electronic record systems in contexts other than the provision of healthcare services. It will be further recognised that the invention is equally applicable to portable personal computing devices of various kinds issued by other kinds of entities.

With reference to Figure 1, a system of issuing suitable portable personal computing devices and associated Public Key Certificates is detailed. In the preferred embodiment each said portable personal computing device is a chip-enabled Health ID Card 10 issued by an authoritative entity 50 to a Patient 1. Each Health ID Card 10 has human readable printed information 11 on its surface pertaining to the identity of the Patient 1, and an Integrated Circuit 12 capable of storing one or more asymmetric cryptographic Private Keys. In the preferred embodiment the Health ID Card

issuer 50 distributes each Health ID Cards 10 in an initial state where no said Private Key has yet been issued to the Patient 1.

At some time after receiving their Health ID Card 10, Patient 1 attends a Registration Authority 41. The Registration Authority 41 is associated with a Certification Authority 30. The Registration Authority 41 is responsible for verifying the personal identity and entitlements of the Patient 1 and, if said identity and entitlements are satisfactorily verified, requesting of the Certification Authority 30 that a Public Key Certificate be issued to Patient 1. The Certification Authority 30 has operational elements including a Certification Authority Server 31 which creates Public Key Certificates and a Repository 32 which stores copies of Public Key Certificates and other related information made generally available to users of the system.

The Registration Authority 41 performs its functions with the aid of a Registration Authority Workstation 41, being a computer system with communications interfaces to both the Health ID Card Integrated Circuit 12 and the Certification Authority 31. In keeping with commonly understood principles of Public Key Infrastructure, after Key Pair generation, the asymmetric cryptographic Private Key is stored within the Health ID Card Integrated Circuit 12 while a copy of the asymmetric cryptographic Public Key is transmitted in the form of a Public Key Certificate Request 33 by the Registration Authority Workstation 40 over a Communications Network 99 to the Certification Authority Server 31. The Certification Authority Server 31 processes the Public Key Certificate Request 33, creates an Anonymous Public Key Certificate containing no identity information pertaining to Patient 1, publishes a copy of said Anonymous Public Key Certificate on the Repository 32, and transmits a copy of said Anonymous Public Key Certificate back to the Registration Authority Workstation 40. While said Anonymous Public Key Certificate contains no identity information pertaining to Patient 1, it does contain the value of a numerical Unique Patient Identifier corresponding to Patient 1. Said numerical Unique Patient Identifier serves as an electronic record pointer to index information on Patient 1 from within an electronic health record system.

In its preferred embodiment the invention provides for an alternative method for authorised healthcare providers to obtain access under prescribed conditions to a copy of a Unique Patient Identifier as stored within the Anonymous Public Key Certificate of a given Non-Competent Patient without it being necessary for the Health ID Card of said Non-Competent Patient to be pass-

phrase activated. Referring to Figure 1, said alternative method in this preferred embodiment comprises the steps of:

- At the time said Anonymous Public Key Certificate containing a said Unique Patient Identifier is created and issued to Patient 1, a copy of said a Unique Patient Identifier is made.
- A Digital Data Item is made comprising said a Unique Patient Identifier and a copy of the name of Patient 1 and/or other identity information sufficient to uniquely identify Patient 1 within the electronic health record system.
- Said Digital Data Item is encrypted using an asymmetric cryptographic Public Key belonging to a trusted Emergency Unique Patient Identifier Recovery entity 80.
- Said Encrypted Digital Data Item 83 is transmitted to the Emergency Unique Patient Identifier Recovery entity 80.
- On receipt of Encrypted Digital Data Item 83 the Emergency Unique Patient Identifier Recovery entity 80 uses an Access Control function 81 to verify the source of the data and stores said encrypted data in secure memory Store 82, for later use.

With reference to Figure 2, systems for utilising the Health ID Card 10 and associated Anonymous Public Key Certificate to update electronic health records are detailed. When attending a Healthcare Provider 200 the Patient 1 presents their Health ID Card 10 to a Clinical Work Station 201 and activates the asymmetric cryptographic Private Key(s) controlled by the Health ID Card 10 by correctly entering a secret pass-phrase. It will be appreciated by persons skilled in electronic security systems that once a Private Key controlled by the Health ID Card 10 has been so activated, the Access Control function 101 can verify through a variety of means that the Patient 1 attending the Clinical Workstation 201 is the same Patient to whom any given digitally signed data item applies. In this preferred embodiment, such verification is performed by Access Control 101 extracting from the Public Key Certificate associated with said given digitally signed data item the associated asymmetric cryptographic Public Key, creating an asymmetric cryptographic challenge using said Public Key, and transmitting said challenge to the Clinical Workstation 201. The Clinical Workstation 201 then responds to said challenge using the asymmetric cryptographic Private Key of Patient 1 as controlled by Health ID Card 10 and transmits its response to the Access Control 101. If the response received by Access Control 101 correctly matches the challenge then Access Control 101 can proceed to grant access to the Clinical Workstation 201 on the basis that the Health ID Card 10 has been shown to control the same asymmetric cryptographic Private Key as was used to create Digital Signature codes on said data items.

Subsequently, under the control of software in Clinical Workstation 201, new data items created by Healthcare Provider A 201 pertaining to Patient 1 are digitally signed using the asymmetric cryptographic Private Key of Patient 1 before being transmitted 103 to associated Electronic Health Record A 100. At a different time when Patient 1 attends a different Healthcare Provider B 210, similar processes of digitally signing data items under the control of Clinical Workstation B 211 are undertaken in relation to what in the case of Figure 2 is a separate Electronic Health Record B 110.

Although it is beyond the scope of the current invention, it is noted that the rights of any given healthcare provider with a direct clinical interest in a given patient to access certain records pertaining to said patient will typically be governed by access control rules designed for the electronic record system in question. Said access control rules are expressed in software in Access Control 101 and Access Control 111 for respective Electronic Health Record systems shown in Figure 2.

With reference to Figure 3, systems for anonymously accessing electronic health records pertaining to a given patient are detailed. Shown are a Public Health Researcher 300 and a Health Policy Analyst 310 who have interests in information stored in Electronic Health Record 120 pertaining to patients identified anonymously by Unique Patient Identifier X 15 and Unique Patient Identifier Y 16. The rights of Researcher 300 and Analyst 310 to access certain records pertaining to patients in whom Researcher 300 and Analyst 310 have no direct clinical interest are governed by access control rules expressed in software in Access Control 131. The present invention prevents Researcher 300 or Analyst 310 determining the identity of any patients from knowledge of said patients' Unique Patient Identifiers and/or access to data items from Electronic Health Record 120 digitally signed by said patients using their respective Health ID Cards.

With reference to Figure 4, one system for authorised healthcare providers to gain access under prescribed emergency conditions to the electronic health records of non-competent patients is detailed. While the details of emergency access are outside the scope of the present invention, an illustration of one method of emergency access is provided here only to demonstrate, without limitation, the feasibility of emergency access when ordinarily a patient is only linked to their Unique Patient Identifier via their Health ID Card. In said illustration Emergency Room Doctor 220 is seeking to treat a Non-Competent Patient 2. Even if the Health ID Card 10 of Non-Competent Patient 2 is present, it cannot be activated if the patient is unable to enter their secret pass-phrase. Therefore the Health ID Card Integrated Circuit 13 is inactive and not accessible by

the Hospital Workstation 221. The Doctor 2 however is able to identify the Non-Competent Patient 2 by name and/or additional identity information visible on the Health ID Card 10 or known by other means.

Emergency Unique Patient Identifier Recovery 80 is accessible to authorised Doctor 220 via Access Control 80. Note that the access control rules expressed in Access Control 80 are outside the scope of the present invention. After successful verification of the Doctor 220 by Access Control 80 and presentation of the Name 84 and/or other identity information of Non-Competent Patient 2, an encrypted copy 85 of the Name together with associated Unique Patient Identifier is transmitted back to the Hospital Workstation 221. The data is decrypted at the Hospital Workstation 221 and thereafter data pertaining to Non-Competent Patient 2 can be indexed within the Electronic Health Record 130 using the recovered Unique Patient Identifier.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as described in the specific embodiments disclosed herein, without departing from the spirit or scope of the invention as broadly described. It will be particularly appreciated that the present invention while described in its preferred embodiment as relating to electronic health record applications is equally well suited to other systems of electronic records and electronic transactions where the persons who are the subjects of said records may be identified using smartcards or similar identity devices and where said persons may be issued with Anonymous Public Key Certificates. It will be further appreciated that while the described preferred embodiment utilises smartcards with integrated storage of asymmetric cryptographic Private Keys, the invention is equally suited to other types of portable personal computing devices with integrated storage of asymmetric cryptographic Private Keys, and to further types of portable personal computing devices wherein said Private Keys are stored external to said computing devices but remain under the control of said computing devices. The present embodiments are therefore to be considered in all respects as illustrative and not restrictive.

Title

Means and method of issuing Anonymous Public Key Certificates for indexing electronic record systems.

The claims defining the invention are as follows:

1. A method of issuing Public Key Certificates to Registered Persons within an electronic record system, said method comprising the steps of:
- Issuing on behalf of each Registered Person whose personal information is held within an electronic record system a portable personal computing device with the ability to control the storage of one or more asymmetric cryptographic Private Keys.
- Visibly printing upon the surface of said personal computing device human readable identity information pertaining to said Registered Person.
- Generation of at least one pair of matching asymmetric cryptographic Private and Public Keys.
- Storage of at least one of said asymmetric cryptographic Private Keys under the control of said portable personal computing device.
- Creation on behalf of each said Registered Person a Public Key Certificate for each asymmetric cryptographic Public Key which matches each said asymmetric cryptographic Private Key stored under the control of said portable personal computing device.
- Inclusion in one or more of said Public Key Certificates one or more electronic record pointers with which personal information pertaining to said Registered Person may be indexed within said electronic record system.
- Issuance of said Public Key Certificate(s) to said Registered Persons.

2. A method according to claim 1 wherein said asymmetric cryptographic Private Key is stored within said portable personal computing device.

3. A method according to claim 1 wherein said asymmetric cryptographic Private Key is stored in an external computer system separate from the portable personal computing device where said external computer system is accessed under the control of said portable personal computing device.

4. A method according to any one of claims 1 to 3 wherein said portable personal computing device is a smartcard.

5. A method according to any one of claims 1 to 4 wherein said Public Key Certificate does not contain the name of said Registered Person to whom said Public Key Certificate has been issued.

6. A method according to any one of claims 1 to 5 wherein said Public Key Certificate does not contain any identity information pertaining to said Registered Person to whom said Public Key Certificate has been issued.

7. A method according to any one of claims 1 to 6 where a plurality of asymmetric cryptographic Private Keys are stored under the control of said portable personal computing device and Public Key Certificates corresponding respectively to different said asymmetric cryptographic Private Keys issued by a plurality of entities.

8. A method according to any one of claims 1 to 7 wherein said portable personal computing devices with associated asymmetric cryptographic Private Key storage are initially distributed without Private Keys being yet stored under the control of said personal computing devices.

9. A method according to any one of the preceding claims wherein Digital Signature codes are created for given data items within said electronic record system in order to explicitly link each said digitally signed data item to the value of an electronic record pointer contained in a Public Key Certificate issued to said Registered Person and associated with said Digital Signature codes.

10. A method according to any one of the preceding claims wherein verification using said Public Key Certificate of a given Digital Signature code for a given data item in said electronic record system is used to evince the association of said data item with an electronic record pointer value contained in said Public Key Certificate.

11. A method according to any one of the preceding claims wherein Digital Signature codes are created for given data items in said electronic record system using an asymmetric cryptographic Private Key issued to said Registered Person where each said Digital Signature code is interpreted as explicitly recording the consent of said Registered Person to the creation of each respective digitally signed said data item.

12. A method according to any one of the preceding claims wherein access to an electronic record system is granted to the holder of a portable personal computing device based on the success of an asymmetric cryptographic challenge-response where the challenge utilises the Public Key associated with digitally signed data items contained in said electronic record system and the response utilises a Private Key controlled by said portable personal computing device.

13. A method according to any one of the preceding claims wherein Public Key Certificates associated with one electronic record system are issued corresponding to respective asymmetric cryptographic Private Keys stored under the control of portable personal computing devices issued by a plurality of entities.

14. A method according to any one of the preceding claims wherein said portable personal computing device is a government issued identity card.

15. A method according to any one of the preceding claims wherein said portable personal computing device is a government issued entitlement card.

16. A method according to any one of the preceding claims wherein said portable personal computing device is issued by a financial institution to a customer of said financial institution.

17. A method according to any one of the preceding claims wherein said portable personal computing device is issued on behalf of a financial institution to a customer of said financial institution.

18. A method according to any one of the preceding claims wherein said portable personal computing device forms part of a government issued travel document.

19. A method according to any one of the preceding claims wherein said portable personal computing device is a vehicle driver licence.

20. A method according to any one of the preceding claims wherein said portable personal computing device is a business licence.

21. A method according to any one of the preceding claims wherein said portable personal computing device is issued by or on behalf of a commercial organisation to one of its customers.

22. A method according to any one of the preceding claims wherein said portable personal computing device is issued by or on behalf of an educational institution to a student.

23. A method according to any one of the preceding claims wherein said portable personal computing device is issued by or on behalf of an employer to one of its employees.

24. A method according to any one of the preceding claims wherein said portable personal computing device is issued by or on behalf of an association to one of its members.

25. A method according to any one of the preceding claims wherein said portable personal computing device is a subscriber identification module within a mobile telephone.

26. A method according to any one of the preceding claims wherein said portable personal computing device is a subscriber identification token associated with a subscription television set-top box.

27. A method according to any one of the preceding claims wherein said portable personal computing device is a road toll identification device.

28. A method according to any one of the preceding claims wherein said portable personal computing device is a radio frequency identification tag.

29. A method according to any one of the preceding claims wherein said electronic record system is for the purpose of recording votes in an electoral system cast by the Registered Person to whom said portable personal computing device has been issued.

30. A method according to any one of the preceding claims wherein said electronic record system is for the purpose of undertaking commercial transactions with the Registered Person to whom said portable personal computing device has been issued.

31. A method according to any one of the preceding claims wherein said electronic record system is for the purpose of accounting for the movements of the Registered Person to whom said portable personal computing device has been issued.

32. A means for issuing Public Key Certificates to Registered Persons within an electronic record system, said means comprising the elements of:
- One or more portable personal computing devices with the ability to control the storage of one or more asymmetric cryptographic Private Keys.
- A recognised authoritative entity to issue said portable personal computing devices to Registered Persons about whom personal information is held within said electronic record system.
- Human readable identity information pertaining to said Registered Persons visibly printed on the surface of respective said portable personal computing devices.
- A key generation system to create at least one pair of asymmetric cryptographic Private and Public Keys for each said Registered User.
- A Public Key Certificate issued to each said Registered Person corresponding to each said asymmetric cryptographic Private Key stored under the control of said portable personal computing devices.
- At least one electronic record pointer contained within the data contents of each said Public Key Certificate where said electronic record pointer may be used to index records within said electronic record system pertaining to the Registered Person to whom each said Public Key Certificate has been issued.
- A Certification Authority which creates said Public Key Certificates for said Registered Persons.

33. A means according to claim 32 wherein Digital Signature codes created for given data items within said electronic record system are interpreted as explicitly linking each said digitally signed data item to the value of an electronic record pointer contained in a Public Key Certificate issued to said Registered Person and associated with said Digital Signature codes.

34. A means according to either of claims 32 or 32 wherein the verification using said Public Key Certificate of a given Digital Signature code for a given data item in said electronic record system is interpreted to evince the association of said data item with an electronic record pointer value contained in said Public Key Certificate.

35. A means according to any one of claims 31 to 33 wherein Digital Signature codes created for given data items in said electronic record system using an asymmetric cryptographic Private Key issued to said Registered Person are interpreted as recording the consent of said Registered Person to the creation of each respective digitally signed said data item.

36. A computer system substantially as herein described with reference to the accompanying figures.

Title

Means and method of issuing Anonymous Public Key Certificates for indexing electronic record systems.

Abstract

The invention herein disclosed provides a method for issuing Anonymous Public Key Certificates to Registered Persons in an electronic record system, where pointers for indexing said record system are stored within said Anonymous Public Key Certificates, and where associated Private Keys are controlled by smartcards or similar devices. Electronic records may be identifiably indexed when the smartcard or similar device has been activated by its holder correctly entering their secret pass-phrase, or anonymously indexed when only the value of a pointer is known.

The only direct linkage between each said Anonymous Public Key Certificate and the Registered Person to whom said Anonymous Certificate is issued is through the associated Private Key as controlled by a smartcard or similar device. Using this invention the retrieval of identifiable records pertaining to a given Registered Person from an electronic record system is normally only possible with the agency of said Person's smartcard or similar device, and therefore normally only possible with said Person's consent.

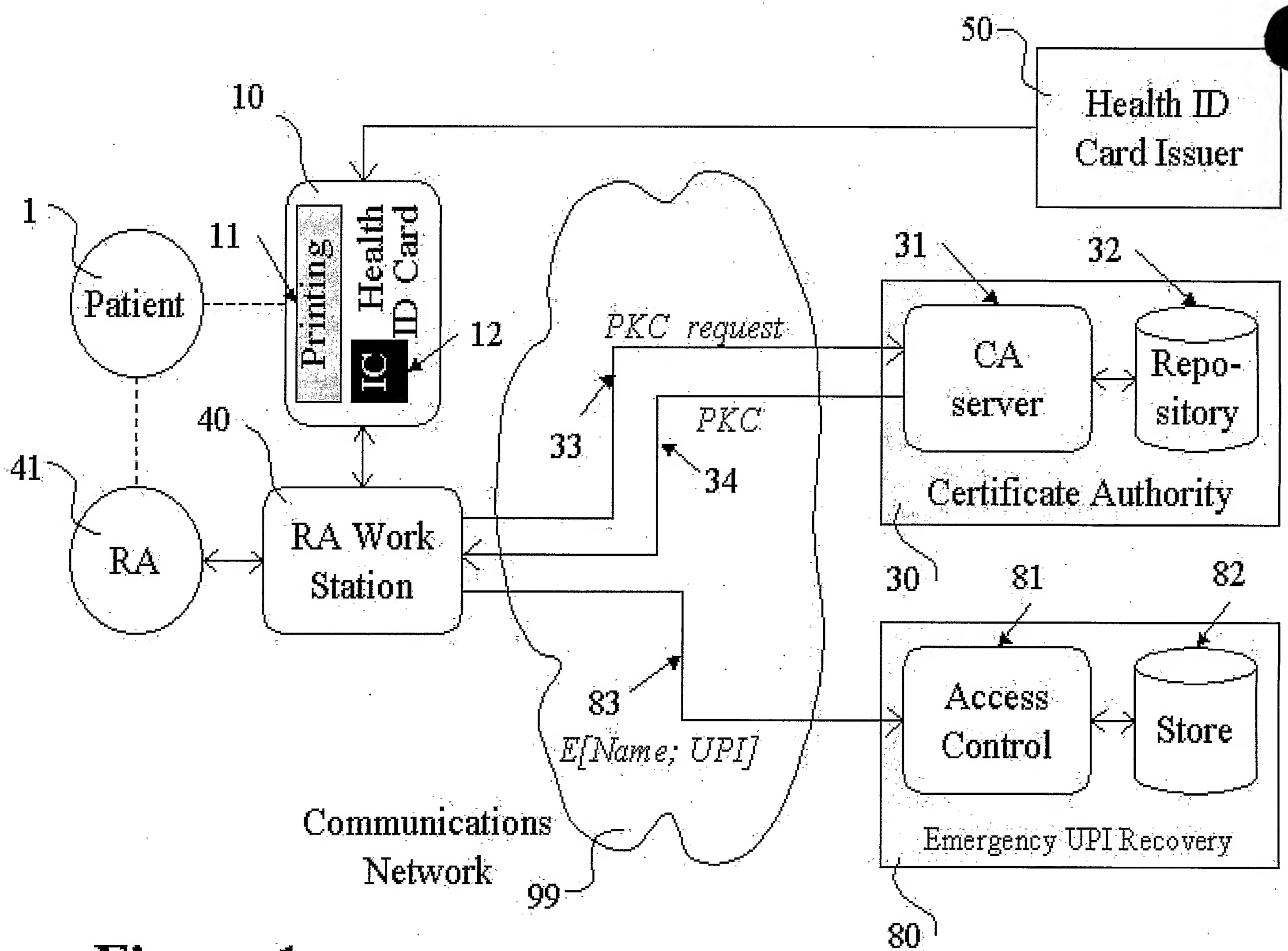
50
Health ID
Card Issuer
10
1
Patient
11
Printing
Health
ID Card
IC
12
40
41
RA
RA Work
Station
PKC request
33
PKC
34
31
32
CA
server
Repo-
sitory
Certificate Authority
30
81
82
Access
Control
Store
Emergency UPI Recovery
83
E[Name; UPI]
Communications
Network
99
80

Figure 1

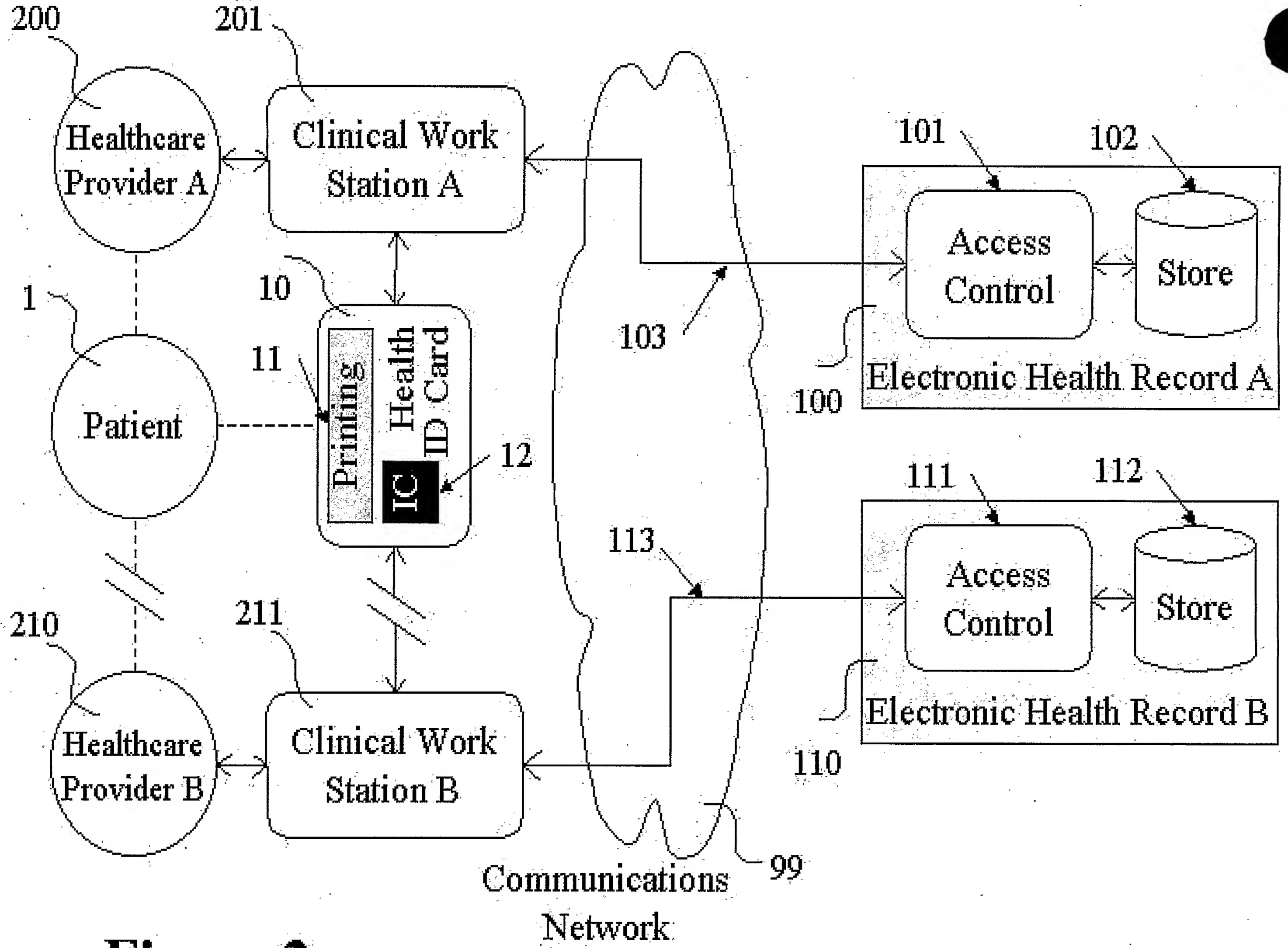
200
201
Healthcare Provider A
Clinical Work Station A
101
102
Access Control
Store
Electronic Health Record A
100
1
10
11
Patient
Printing
Health ID Card
IC
12
103
111
112
113
Access Control
Store
Electronic Health Record B
110
210
211
Healthcare Provider B
Clinical Work Station B
99
Communications Network

Figure 2

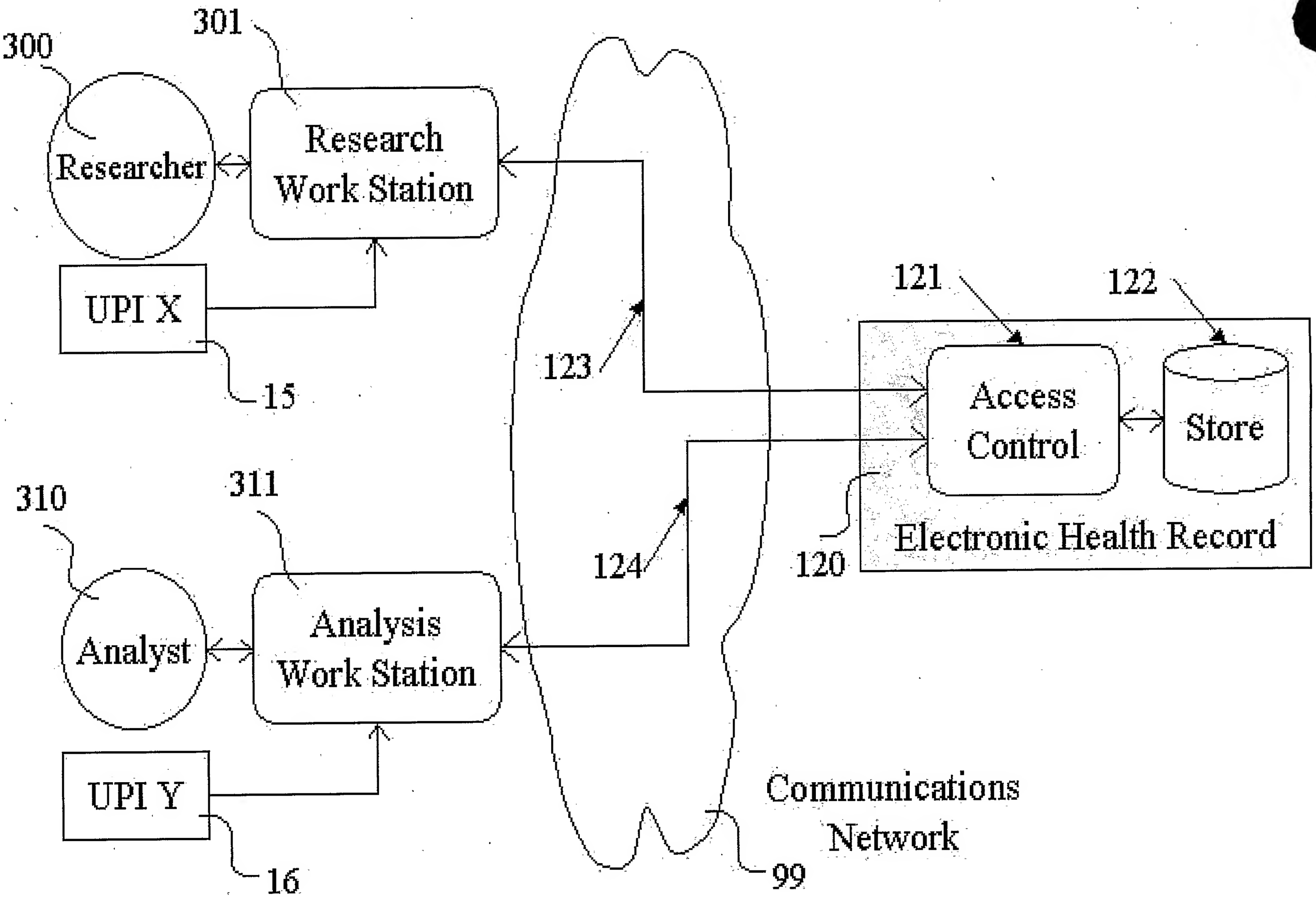
300
301
Researcher
Research
Work Station
UPI X
15
123
121
122
Access
Control
Store
Electronic Health Record
120
124
310
311
Analyst
Analysis
Work Station
UPI Y
16
Communications
Network
99

Figure 3

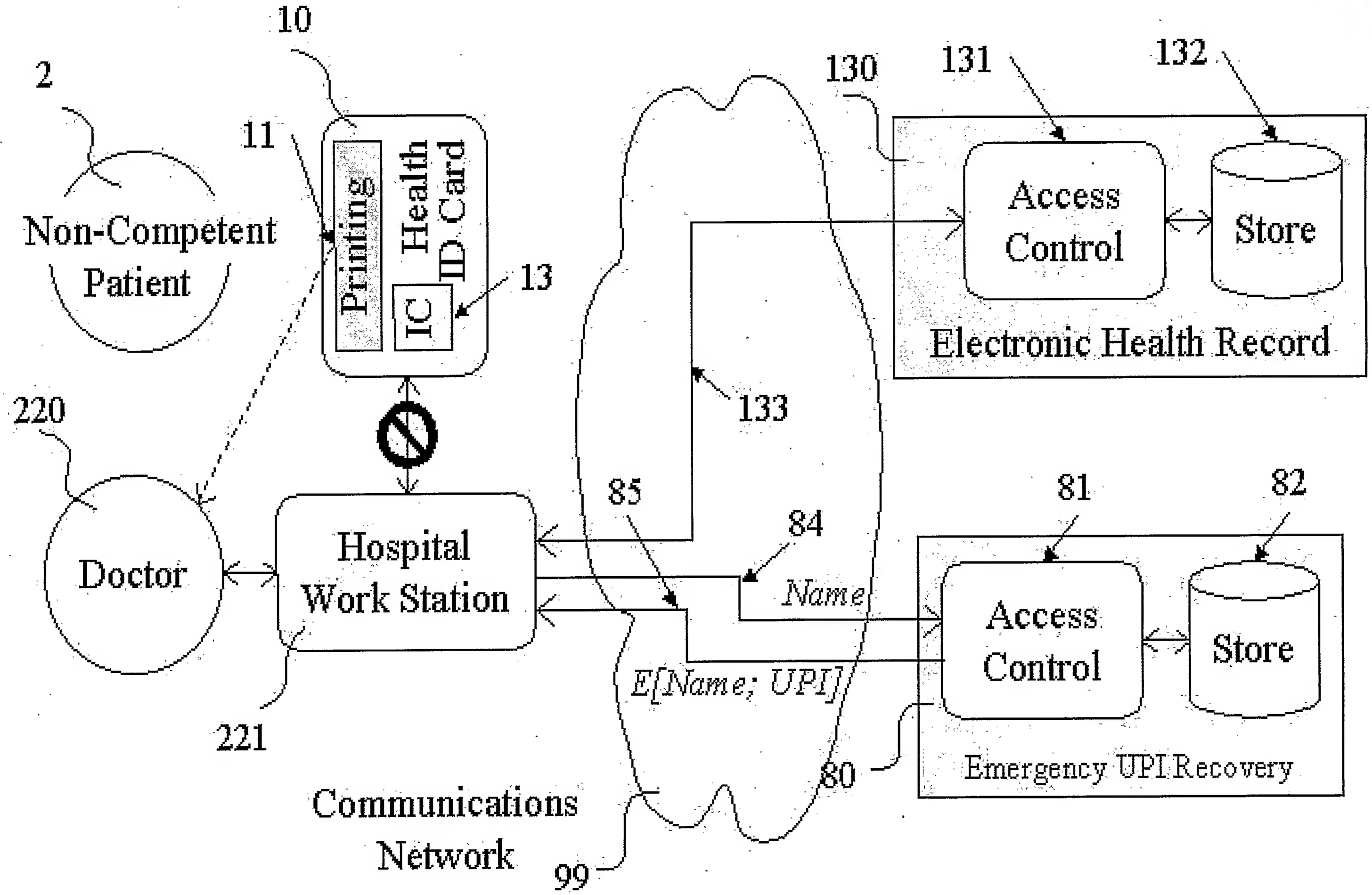
10
2
11
Non-Competent
Patient
Printing
Health
ID Card
IC
13
130
131
132
Access
Control
Store
Electronic Health Record
133
220
85
81
82
84
Doctor
Hospital
Work Station
Name
Access
Control
Store
E[Name; UPI]
221
80
Emergency UPI Recovery
Communications
Network
99

Figure 4